UNITED STATES DISTRICT COURT

for the

District of Massachusetts

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple ID hugogmbrazil@gmail.com iCloud Account and Associated Data

Case No. 22-mj-7357-JCB

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

Please See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
8 USC 1324(a)(1)(A) & (B)(1)	Bringing in and harboring certain aliens for commercial advantage or private financial gain; hiring for employment 10 or more aliens in a 12-month period.
8 USC 1324 (a)(3)(A)	
18 USC 1956(a) & (h)	Concealment and international promotion money laundering and conspiracy.

The application is based on these facts:

See Attached Affidavit of DOL-OIG OI Special Agent Sean P. Roberts

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sean P. Roberts
Applicant's signature

Sean P. Roberts, DOL-OIG OI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 11/30/2022

City and state: Boston, MA

UNITED STATES DISTRICT COURT DISTRICT OF MASSACHUSETTS

Judge's signature

Hon. Jennifer C. Boal, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A – APPLE

The premises to be searched and seized are: (1) the iCloud account identified as: Apple ID hugogmbrazil@gmail.com (the "Target Account"); (2) other user-generated data stored with this account, including the contents of communications; and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Apple, Inc., ("Apple"), which accepts service of process at:

Apple Litigation Group
Apple, Inc.
1 Infinite Loop M/S 169-NYJ
Cupertino, CA 05014-2084
lawenforcement@apple.com

ATTACHMENT B – APPLE INC.

I. Search Procedure

A. Within fourteen days of the search warrant's issue, the warrant will be served on Apple, which will identify the accounts and files to be searched, as described in Section II below.

B. Apple will then create an exact electronic duplicate of these accounts and files ("the account duplicate").

C. Apple will provide the account duplicate to law enforcement personnel.

D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.

E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created by Apple after fourteen days from the warrant's issue ("late-created data"), law enforcement personnel may view any late-created data, including subscriber, IP address, logging, and other transactional data that was created by Apple without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

II. Information to Be Disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of APPLE, including any messages, records, files, logs, documents or

information that have been deleted but are still available to APPLE, including all iOS backups and all Apple and third-party application data, or have been preserved pursuant to a request made under 18 U.S.C § 2703(f), APPLE is required to disclose the following information to the government, in unencrypted form whenever available, corresponding to the account or identifier ("Account") listed in Attachment A:

a. *Message content*: For the period between July 1, 2016 and October 3, 2022, the contents of all communications and related transactional records for all APPLE services used by the Account subscriber/user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services), including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies). Contents of all other data and related transactional records for all Apple services used by the Account user including all messages sent to or from, stored/backed-up in draft form in, or otherwise associated with the Account, including all message content (to include e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services, iOS stored/backed-up voice content), attachments, and header information (specifically including the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message);

b. *Instant Messages*: For the period between July 1, 2016 and October 3, 2022, The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

c. *iCloud Data*: For the period between July 1, 2016 and October 3, 2022, The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, and iCloud Drive. The contents of all other data to include audio files and voice data and related transactional records for all APPLE services and third-party applications/services used by the Account user, including any and all information generated, modified, or stored by user(s) or APPLE in connection with the Account (such as contacts, calendar data, images, videos, notes, audio files, voice notes, third-party application/service data, Apple and third-party telephone call recorder application data, third-party messenger application data, documents, bookmarks, profiles, device backups, and any other saved information);

d. *Images, videos, audio, documents and files:* All pictures, videos, audio, documents, and files posted and/or stored by the Account user, including metadata and geotags;

e. *Address book information*: All address book, contact list, or similar information associated with the Target Account;

f. *Other stored electronic information*: All records/data and other information stored/backed-up to include Apple and third-party messenger application data such as WhatsApp

(text) messages, WhatsApp media (video), WhatsApp voice messages (audio files), WhatsApp documents, and WhatsApp contacts;

g. For the period between July 1, 2016 and October 3, 2022: All APPLE records concerning the online search and browsing history associated with the Account or its users (such as information collected through tracking cookies);

h. For the period between July 1, 2016 and October 3, 2022: All records and other information concerning any document, or other computer files created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

i. All records regarding identification of the Account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;

j. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access APPLE services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers

("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

k. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any APPLE account (including both current and historical accounts) ever linked to the Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (*e.g.*, credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

l. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

m. For the period between July 1, 2016 and October 3, 2022: All records of communications between APPLE and any person regarding the Account, including contacts with support services and records of actions taken;

n. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to APPLE (including, but not limited to, the keybag.txt and fileinfolist.txt files);

o. Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to the Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Account or associated user(s) (but not including confidential communications with legal counsel);

p. *Find My iPhone and Remote Deletion Activity*: All find My iPhone connection logs and Find My iPhone transactional activity for requests to remotely lock or erase or wipe a device;

q. *Service information*: The types of services utilized by the user of the Target Account;

r. *Linked Accounts*: All accounts linked to the Target Account (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, Apple ID, or otherwise;

s. *Preserved or backup records:* Any and all preserved or backup copies of any of the foregoing categories of records to include voice data (to include Apple and third-party application voice/call recording data), whether created in response to a preservation request issued pursuant to 18 United States Code, Section 2703(f) or otherwise to include any and all messenger application data to include third-party messenger application data such as WhatsApp; and

t. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

u. Within 14 days of the issuance of this warrant, Apple shall deliver the information set forth above via United States mail, courier, or e-mail to the following:

Sean P. Roberts
Special Agent
U.S. Department of Labor-Office of Inspector General, Office of Investigations
675B New Sudbury Street
Boston, MA 02203
roberts.sean@oig.dol.gov

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

A. Evidence, fruits, or instrumentalities of violations of offenses including alien smuggling in violation of 8 U.S.C. §§ 1324(a)(1)(A)(i) and (B)(1); and §§ 1324(a)(1)(A)(iv) and (B)(1); conspiracy and aiding and abetting the same in violation of 8 U.S.C. § 1324(a)(1)(A)(v)(I) and (B)(i); hiring unauthorized aliens in violation of 8 U.S.C. § 1324(a)(3)(A); money laundering in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(a)(2)(A); and money laundering conspiracy in violation of 18 U.S.C. § 1956(h), including:

B. Evidence pertaining to the following people, entities, physical addresses, telephone numbers, e-mail addresses, websites, and social media accounts:

1. **CHELBE** WILLAMS MORAES (DOB 05/16/1961)
2. Phone number +55 31 9727 3586
3. **JESSE** JAMES MORAES (DOB 01/13/1958)
4. Phone number 781-879-0068
5. **HUGO** GIOVANNI MORAES (DOB 10/22/1979)
6. Phone number 781-858-4830
7. **CAROLINE** DE MORAES PARLEE (DOB 10/05/1988)
8. Phone number 781-608-5201

9. **JANAINA** DE MORAES GUALBERTO (DOB 04/09/1994)

10. Phone number 781-640-3632

11. **TASTE OF BRAZIL**—TUDO NA BRASA, LLC, 414 Main Street, Woburn, MA

12. **THE DOG HOUSE** BAR & GRILL, LLC, 434 Main Street, Woburn, MA (together with **TASTE OF BRAZIL, the RESTAURANTS**);

13. 37 Center Street, Woburn, MA

14. hugogmbrazil@gmail.com

15. hugo@thedoghousewoburn.com

16. 434mainstreet@gmail.com

17. loredanna_18@msn.com

18. carolinemoraesbh@hotmail.com

19. Website, Facebook, and Instagram accounts for **THE DOG HOUSE**

20. Website, Facebook, and Instagram accounts for **TASTE OF BRAZIL**

C. Evidence pertaining to the following topics:

1. Identification of employees of the **RESTAURANTS**, such as a list of employees and job duties, employees' names, aliases, addresses, phone numbers, dates of birth, social security numbers and taxpayer identification numbers, identification documents, and applications and employment contracts.

2. Employees' immigration and work authorization/verification, such as copies of identification documents provided by or on behalf of employees, documents executed by employees and **RESTAURANTS'** supervisors or

managers, documents submitted to federal, state and local authorities, and communications.

3. The **RESTAURANTS**' payroll and scheduling records, such as employees' shift schedules, assigned jobs, time cards, records of hours worked, records of payment in any form *(i.e.*, check, cash, debit card, in-kind, satisfaction of debt, etc.), documents submitted to federal, state, and local authorities, and communications.

D. Evidence pertaining to the payment, receipt, transfer, or storage of money or other things of value by or to any one of the names listed above, including, without limitation:

1. Bank, credit union, investment, money transfer, and other financial accounts;

2. Credit and debit card accounts;

3. Tax statements and returns;

4. Business or personal expenses;

5. Income, whether from wages or investments; and

6. Loans.

E. Evidence pertaining to the travel or whereabouts of **CHELBE** WILLAMS MORAES, **JESSE** JAMES MORAES, **HUGO** GIOVANNI MORAES, **CAROLINE** DE MORAES PARLEE, and **JANAINA** DE MORAES GUALBERTO between July 1, 2016 and the present;

F. Evidence pertaining to the existence, identity, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;

G. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

H. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);

I. Evidence of the geographic location of user of the Target Account, as well as the computers or devices used to access the Target Account, with respect to information maintained by the Provider relating to GPS, Wi-Fi, cell site location, and mobile networks;

J. Other e mail or Internet accounts providing Internet access or remote data storage;

K. The existence or location of physical media storing electronic data, such as hard drives, CD or DVD ROMs, or thumb drives;

L. The existence or location of paper print outs of any data from any of the above; and

M. Evidence pertaining to any computer hardware, computer software, mobile phones, or storage media related to the Target Account ("the computer equipment"), including:

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;

5. evidence of when the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and

7. evidence pertaining to accounts held with companies providing Internet access or remote storage.

DEFINITIONS

For the purpose of this warrant:

N. “Computer equipment” means any computer hardware, computer software, mobile phone, storage media, and data.

O. “Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

P. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

Q. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

R. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

S. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.